Classical codes in quantum state space

Mark Howard[1]

[1] *Institute for Quantum Computing and Department of Applied Mathematics, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1*

We present a construction of Hermitian operators and quantum states labelled by strings from a finite field. The distance between these operators or states is then simply related (typically, proportional) to the Hamming distance between their corresponding strings. This allows a straightforward application of classical coding theory to find arrangements of operators or states with a given distance distribution. Using the simplex or extended Reed-Solomon code in our construction recovers the discrete Wigner function, which has important applications in quantum information theory.

I. OVERVIEW

Figure 1(a) depicts the binary Hamming cube – all binary strings of length 3 where strings that differ by one element are one edge length apart, strings differing by two elements are two edge lengths apart etc. The number of differing elements between two strings is the Hamming distance and finding useful arrangements of q-ary strings (with prescribed mutual Hamming distances) is the subject of classical coding theory. Let $q = p^n$ denote an integer that is a prime power. We will present a construction that associates q-ary strings with (i) Hermitian operators in Hilbert space of dimension $\dim(\mathcal{H}) = q$, and (ii) pure states in $\mathcal{H}^{\otimes 2}$. We find a remarkably simple relationship between the Hamming distance of strings and the Hilbert-Schmidt or Fubini-Study distance of the corresponding operators or states, respectively. Because of the array of powerful coding-theoretic tools at our disposal, our construction may be useful for finding arrangements of quantum states or operators that would otherwise not be apparent.

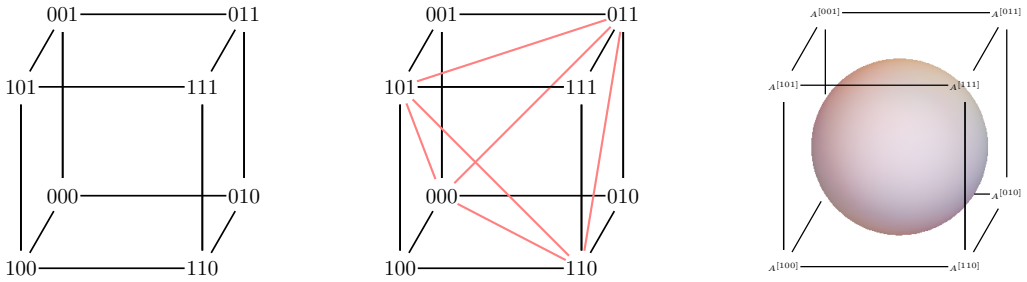


FIG. 1. (a) Hamming cube for binary vectors of length 3, (b) the simplex code $\mathcal{C} \subset \mathbb{F}_2^3$ inscribed within it and (c) the facet operators A^r corresponding to $r \in \mathbb{F}_2^3$ and their geometrical relationship to the Bloch ball (the subset of Hermitian operators corresponding to valid quantum states) for a single qubit.

Figure 1(b) depicts the so-called simplex code, which is one member of family of q-ary codes that is well-defined for all prime powers q. Applying our construction to the codewords of this code (i.e., the vertices of the inscribed simplex) we find a set of operators that correspond to the phase point operators of Wootters' discrete Wigner function. States that have non-negative quasi-probability representation in this Wigner function correspond to states that are not too far from any of the operators associated with the codewords of the code (see Fig. 2). This perspective on the Wigner function and its relationship with quantum state space may prove enlightening.

II. MUBS AND FACE OPERATORS

We will adopt the notation of quantum information theory so that the standard basis has elements $|k\rangle := \mathbf{e}_k \in \mathbb{C}^q = \mathcal{H}$ and $\langle\cdot|\cdot\rangle$ is the inner product on $\mathcal{H}$. Given an orthonormal basis $\mathcal{B} = \{|0\rangle, \ldots, |q-1\rangle\}$, a unit vector $|v\rangle$ is called unbiased if $|\langle v|k\rangle| = \frac{1}{\sqrt{q}}$ for all $0 \leq k \leq q-1$. We will focus on Hilbert spaces of prime power dimension q where it is known that $q+1$ (the maximal possible number) mutually unbiased bases always exist. For non-prime-power dimensions the number of MUBs is lower bounded by the largest component in a prime decomposition of $\dim(\mathcal{H})$, but this is typically much lower than $\dim(\mathcal{H})+1$. In subsequent sections we will be interested in connections between

MUBs and classical coding theory so we find it convenient to label MUB vectors with elements of the finite field, $\mathbb{F}_q$, containing $\dim(\mathcal{H}) = q$ elements. In fact it is quite natural to use $\mathbb{F}_q$ since many MUB constructions already use finite fields [1–3] so that e.g. Gauss sums can be used to prove the required overlap constraints. A complete set of MUBs has one more basis than the number of field elements so we label this basis with ∞.

Definition II.1 ***Mutually unbiased bases:*** *A complete set of MUBs in a Hilbert space of dimension $dim(\mathcal{H}) = q$ is given by $q+1$ orthonormal bases $\{\mathcal{B}_\infty, \mathcal{B}_0, \mathcal{B}_1, \ldots\} = \bigcup_{B\in\{\infty,\mathbb{F}_q\}} \mathcal{B}_B$, where each basis comprises $\mathcal{B}_B = \{|\psi_B^V\rangle, V \in \mathbb{F}_q\}$, and overlaps obey*

$$|\langle\psi_B^V|\psi_{B'}^{V'}\rangle| = \frac{1}{\sqrt{q}}(1-\delta_{B,B'}) + \delta_{B,B'}\delta_{V,V'}. \tag{1}$$

Our results do not depend on the specifics of the mutually unbiased bases that we use. All that matters is their defining characteristic i.e., the pairwise inner products encapsulated in Eq. (1). In that sense, it is unnecessary that MUB vectors be labeled by elements of $\mathbb{F}_q$ since any consistent labeling will do. We suggest that our choice is as convenient as any other and has the additional merit that the labeling is physically meaningful in at least one case, which we discuss in Sec. V. (In the context of quantum information this particular MUB construction is important because all basis vectors are eigenvectors of Pauli/Weyl-Heisenberg operators.) A good survey of different MUB constructions in power-of-prime dimensions is provided by Kantor [4]. Our construction also works without modification if we use a (necessarily incomplete) set of MUBs in $\dim(\mathcal{H}) = p^2$ that exclusively uses entangled basis vectors [5]. The association between Hermitian operators and $\mathbb{F}_q$-valued vectors is given by the following definitions, whose name derives from a geometrical interpretation described in Sec. V.

Definition II.2 ***Facet operators:*** *Using a complete set of mutually unbiased bases $\{|\psi_B^V\rangle, V \in \mathbb{F}_q, B \in \{\infty, \mathbb{F}_q\}\}$ as in Definition II.1, a facet operator indexed by a vector $r \in \mathbb{F}_q^{q+1}$ is defined as*

$$A^{r=[r_\infty,r_0,r_1,\ldots,r_B,\ldots]} = \sum_{B\in\mathbb{F}_q,\infty} |\psi_B^{r_B}\rangle\langle\psi_B^{r_B}| - \mathbb{I}_q. \tag{2}$$

For example in $\dim(\mathcal{H}) = 3$ a possible facet operator A^r with $r = [0, 1, 2, 0]$ corresponds to choosing the zeroth vector from the computational ($\mathcal{B}_\infty$) basis, the first vector in the $\mathcal{B}_0$ basis, the second vector in the $\mathcal{B}_1$ basis and the zeroth vector in the $\mathcal{B}_2$ basis. Dropping the requirement that we select a vector from every basis we arrive at the definition of a Face operator,

Definition II.3 ***Face operators:*** *Using a subset, of cardinality $|r|$ $(1 \le |r| \le q+1)$, of a complete set of mutually unbiased bases, a face operator indexed by a vector $r \in \mathbb{F}_q^{|r|}$, is defined as*

$$A^r = \sum_{\substack{B\subseteq\{\infty,\mathbb{F}_q\}\\ |\{B\}|=|r|}} |\psi_B^{r_B}\rangle\langle\psi_B^{r_B}| - \left(\frac{|r| - \sqrt{q^2 - q|r| + |r|}}{q}\right)\mathbb{I}_q. \tag{3}$$

For example, we could drop the $\mathcal{B}_\infty$ and $\mathcal{B}_1$ bases from the previous example, and then A^r with $r = [r_0, r_2] = [2, 0]$ corresponds to taking the second vector from $\mathcal{B}_0$ and the zeroth vector from $\mathcal{B}_2$. The definition for face operators completely subsumes the previous one since facet operators correspond to the special case $|r| = q+1$. Nevertheless we have given them separate definitions as facet operators are the most interesting, and the simplification of the identity coefficient is not immediately apparent.

III. FINITE FIELDS AND q-ARY CODES

A field is a non-empty set $\mathbb{F}$ of elements with abelian addition and multiplication, satisfying the usual axioms e.g. distributivity. We denote as $\mathbb{F}_q$ the finite field of order $q = p^n$ where p is a prime and $n \ge 1$ is an integer. The smallest number of times the unit element $1 \in \mathbb{F}_q$ must be added to itself to produce 0 is the characteristic of the field, which is p, and consequently any element $\beta \in \mathbb{F}_q$ satisfies $p\beta = 0$. If $n = 1$ and $q = p$ then $\mathbb{F}_q \cong \mathbb{Z}_p := \{0, 1, \ldots, p-1\}$ – the integers modulo p. When $n > 1$ it is necessary to extend $\mathbb{F}_p$ to $\mathbb{F}_q$ with the addition of extra elements but we will not discuss the details of how this achieved. It will be sufficient to note that the nonzero elements of $\mathbb{F}_q$ form a cyclic group of order $q-1$ and a primitive element denoted α generates this whole group – $\mathbb{F}_q/\{0\} = \{\alpha, \alpha^2, \ldots, \alpha^{q-1} = 1\}$.

The 1-dimensional vector space $\mathbb{F}_{p^n}$ is also an n-dimensional vector space over $\mathbb{F}_p$. Let $\mathrm{tr} : \mathbb{F}_{q=p^n} \mapsto \mathbb{F}_p$ be the trace map

$$\mathrm{tr}(\beta) := \sum_{k=0}^{n-1} \beta^{p^k} \tag{4}$$

then a standard result (useful in the context of Weyl Heisenberg operators later) is that for any $\gamma \in \mathbb{F}_q$

$$\sum_{\beta \in \mathbb{F}_q} \omega^{tr(\beta\gamma)} = q\delta_{\gamma,0} \qquad \text{where } \omega := exp(2\pi i/p). \tag{5}$$

A q-ary alphabet, that is a set of q distinct symbols, is naturally identified with elements of the finite field $\mathbb{F}_q$. A word of length N, $w \in \mathbb{F}_q^N$, is a string of N symbols from $\mathbb{F}_q$ and clearly there are q^N distinct words of this fixed length. The most general definition of a q-ary code is as a subset $\mathcal{C} \subseteq \mathbb{F}_q^N$ and the elements of $\mathcal{C}$ are called codewords (a good reference for all coding-related material is [6]). The Hamming distance $0 \leq \Delta(v, w) \leq N$ between two words $v, w \in \mathbb{F}_q^N$ is the number of positions in which v and w disagree. The Hamming distance is a metric on $\mathbb{F}_q^N$ so that expressions like $\Delta(u, w) \leq \Delta(u, v) + \Delta(v, w)$ hold. Using the Hamming distance we can define a ball/sphere of radius r around any word w via $\{v \in \mathbb{F}_q^N | \Delta(v, w) \leq r\}$. Roughly speaking, good codes consist of codewords $\mathcal{C} \subset \mathbb{F}_q^N$ where each codeword is the center of relatively large Hamming sphere, and this set of Hamming spheres fill the whole space without intersecting one another. The minimum distance $d(\mathcal{C})$ of a code is given by $d(\mathcal{C}) = \min\{\Delta(x, y) | x \neq y \in \mathcal{C}\}$, and this is related to the radius of the empty Hamming spheres around each codeword. Two codes $\mathcal{C}$ and $\mathcal{C}'$ are equivalent if they are related by trivial operations like permuting symbols or positions of codewords in a consistent way. Codes can be either linear or non-linear with the former typically being more amenable to analysis and simple encoding procedures. A linear code of length N has q^k codewords for some integer $k \geq 0$ and is denoted $[N, k, d]$, whereas a nonlinear code has M codewords and is denoted (N, M, d). From a purely combinatorial point of view, linear codes may be outperformed by nonlinear codes.

The Hamming bound says that a q-ary code of block length N and distance d has a cardinality $|\mathcal{C}|$ that is upper bounded by following expression

$$\text{Hamming Bound:} \qquad |\mathcal{C}| \leq q^N / \sum_{i=0}^{[\frac{d-1}{2}]} \binom{N}{i} (q-1)^i, \tag{6}$$

and codes that saturate this bound are perfect e.g., the Hamming codes mentioned later. The Singleton bound says that a code $\mathcal{C}$ of block length N and minimum distance d over a q-ary alphabet obeys

$$\text{Singleton Bound:} \qquad |\mathcal{C}| \leq q^{N-d+1}, \tag{7}$$

and codes that saturate this are maximum distance separable [7] (MDS) e.g., the simplex codes mentioned later.

The standard notation for the number of codewords of Hamming weight i from the all zero codeword is

$$A_i = |\{w \in \mathbb{F}_q^N | \Delta(w, 0) = i\}|. \tag{8}$$

and it should not be confused with a face operator (the subscript and context should avoid this issue). The set $\{A_i | 0 \leq i \leq N\}$ is the weight distribution of the code and is calculable using powerful tools like weight enumerators. Clearly for an (N, M, d) code $\sum_{i=0}^{N} A_i = M$.

A code defines a vector space if and only if it is a linear code. A linear code encoding k units of information is described by a generator matrix $G : \mathbb{F}_q^k \mapsto \mathbb{F}_q^N$ e.g., the Simplex code depicted in Fig. 1 has a generator matrix

$$G_{\text{simplex}} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} g_1 \\ g_2 \end{bmatrix}, \tag{9}$$

$$\Rightarrow \ \mathcal{C}_{\text{simplex}} = \{ag_1 + bg_2 | a, b \in \mathbb{F}_2\}, \tag{10}$$

$$= \{(0,0,0), (1,0,1), (0,1,1), (1,1,0)\}. \tag{11}$$

The simplex code is well defined for all prime powers q and for all lengths of the form $N = (q^m - 1)/(q - 1)$ with parameters $[N = (q^m - 1)/(q - 1), k = m, d = q^{m-1}]$. The maximum length of a code that we may use in our construction corresponds to $m = 2$ and we will often refer to this code as *the* simplex code. This simplex code

sometimes goes by the name (doubly) extended Reed-Solomon code. In any event, our simplex code has generator matrix (recall that α is a primitive element of $\mathbb{F}_q$)

$$G_{\text{simplex}} = \begin{bmatrix} 1 & 0 & \alpha & \alpha^2 & \cdots & \alpha^{q-1} \\ 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} g_1 \\ g_2 \end{bmatrix}, \tag{12}$$

$$\Rightarrow \ \mathcal{C}_{\text{simplex}} = \{ag_1 + bg_2 | a, b \in \mathbb{F}_q\}. \tag{13}$$

The simplex code saturates the Singleton bound for all q but only saturates the Hamming bound for $q = 3$ where the simplex code is equivalent to the Hamming code

$$G_{\text{Hamming}} = \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{bmatrix} \qquad (q = 3). \tag{14}$$

The fact that this $q = 3$ code is doubly optimal (both MDS and perfect) arises from the following fact: the simplex code is dual to the Hamming code for all q but these codes coincide (the code is self-dual) for $q = 3$. The Hamming construction describes a family of codes with parameters $[N = (q^m - 1)/(q - 1), k = N - m, d = 3]$ so once again we consider $m = 2$ to describe *the* Hamming code for our purposes. This has a generator matrix with $k = q - 1$ rows i.e.,

$$G_{\text{Hamming}} = \begin{bmatrix} 1 & 0 & 0 & \dots & -\alpha^{q-1} & -\alpha^{q-1} \\ 0 & 1 & 0 & \dots & -\alpha^{q-1} & -\alpha^{q-2} \\ 0 & 0 & 1 & \dots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \dots & -\alpha^{q-1} & -\alpha^2 \\ \vdots & \vdots & \vdots & \dots & -\alpha^{q-1} & -\alpha \end{bmatrix}. \tag{15}$$

For any linear code $\mathcal{C}$ we can define an equivalent code $\mathcal{C}' = \mathcal{C} + w$ by adding a constant offset vector w to each codeword so that both codes have the same distance distribution. A standard coding technique, typically used for decoding, is to partition $\mathbb{F}_q^N$ into cosets of a linear code, where each coset is identified (non-uniquely) by a coset leader w. This decomposition is depicted as a standard or Slepian array as in Table I where we have given an example using the binary simplex code of Fig. 1(b).

Coset leader w	Remainder of $\mathcal{C} + w$		
(0,0,0)	(1,0,1)	(0,1,1)	(1,1,0)
(0,0,1)	(1,0,0)	(0,1,0)	(1,1,1)

TABLE I. Slepian array partitioning $\mathbb{F}_2^3$ into cosets of the binary simplex code (11). The top row corresponds to the vertices of the tetrahedron in Fig. 1(b), whereas the second row consists of the same strings translated by $(0, 0, 1)$. Together the simplex code and its translate exhaust all 8 points of the binary Hamming cube.

IV. DISTANCES IN QUANTUM STATE SPACE

If we start with an operator of the form

$$A^r = \sum_{B \in \mathcal{B}} |\psi_B^{r_B}\rangle\langle\psi_B^{r_B}| - K\mathbb{I}_q \tag{16}$$

then a fairly straightforward counting argument shows that

$$\text{Tr}(A^r) = |r| - qK, \tag{17}$$

$$\text{Tr}\left((A^r)^2\right) = \frac{(q - 1 + |r|)|r|}{q} - 2|r|K + qK^2, \tag{18}$$

$$= q \text{ when } K = \frac{|r| \pm \sqrt{q^2 - q|r| + |r|}}{q}, \tag{19}$$

where the last line explains the somewhat peculiar choice of identity coefficient that we adopted in Def II.3. Observe that face operators are clearly Hermitian $A^r = (A^r)^\dagger$ since each term in the sum is manifestly so. We will examine

the geometrical relationship between these face operators and it is assumed that the same bases are used in the construction of two face operators A^r and A^s. The Hilbert-Schmidt inner product between these operators has remarkably simple expression, which is arguably the key insight of this work:

Lemma IV.1 *Let A^r and A^s be face operators of the form (3), in a Hilbert space of dimension $dim(\mathcal{H}) = q$, then*

$$\mathrm{Tr}\left(A^r A^s\right) = q - \Delta(r,s) \tag{20}$$

where $\Delta(r,s)$ denotes the Hamming distance (number of differing elements) between vectors $r, s \in \mathbb{F}_q^{|r|}$.

Proof Insert the face operator definition from Eq. (3) and use the definition of mutually unbiased bases i.e.,

$$|\langle \psi_B^V | \psi_{B'}^{V'} \rangle|^2 = \frac{1}{q}(1 - \delta_{B,B'}) + \delta_{B,B'}\delta_{V,V'} \tag{21}$$

along with the fact that $\sum_{j=1}^{|r|} \delta_{r_j,s_j} = |r| - \Delta(r,s)$.[1]

Since the operators A^r are elements of the space of bounded linear operators, then the distance between two such operators can be characterized by the Hilbert-Schmidt metric.

Corollary IV.2 *The Hilbert-Schmidt distance between two face operators A^r and A^s of the form (3) is*

$$D_{\mathrm{HS}}\left(A^r, A^s\right) := \sqrt{\mathrm{Tr}[(A^r - A^s)^\dagger (A^r - A^s)]} = \sqrt{2\left[q - \mathrm{Tr}\left(A^r A^s\right)\right]} = \sqrt{2\Delta(r,s)} \tag{27}$$

We can also identify normalized pure quantum states with vectors $r \in \mathbb{F}_q^{|r|}$ by using the Jamiołkowski isomorphism [8, 9] and the distance between quantum states is once again simply related to the Hamming distance,

Corollary IV.3 *Let A^r and A^s be face operators of the form (3), in a Hilbert space of dimension $dim(\mathcal{H}) = q$, then pure states $|J^r\rangle \in \mathbb{C}^{q^2}$ given by $|J^r\rangle = (\mathbb{I} \otimes A^r) \sum_{k \in \mathbb{F}_q} |kk\rangle / \sqrt{q}$ have trace distance and Fubini-Study distance*

$$D_{\mathrm{TR}}\left(|J^r\rangle, |J^s\rangle\right) := \sqrt{1 - |\langle J^r | J^s \rangle|^2} = \frac{1}{q}\sqrt{2q\Delta(r,s) - \Delta^2(r,s)}\ , \tag{28}$$

$$D_{\mathrm{FS}}\left(|J^r\rangle, |J^s\rangle\right) := \sqrt{2 - 2|\langle J^r | J^s \rangle|} = \sqrt{2(1 - |1 - \Delta(r,s)/q|)}\ , \tag{29}$$

where the latter simplifies to $D_{\mathrm{FS}} = \sqrt{2\Delta(r,s)/q}$ whenever $\Delta(r,s) \leq q$.

Proof First note that, although face operators are not unitary in general, the Jamiołkowski isomorph obtained by applying A to one half of a maximally entangled state produces a valid normalized pure state (which is not generally maximally entangled). This can be seen using $\langle J^r | J^r \rangle = \mathrm{Tr}((A^r)^2)/q = 1$ and similarly

$$\langle J^r | J^s \rangle = \mathrm{Tr}(A^r A^s)/q = 1 - \Delta(r,s)/q. \tag{30}$$

The simplex code is equidistant with constant distance $\Delta = q$ between codewords so that $\{|J^r\rangle, r \in \mathcal{C}_{\mathrm{simplex}}\}$ forms a complete orthonormal basis in $\mathbb{C}^{q^2}$.

It is interesting to consider how evenly the set of states $\{|J^r\rangle, r \in \mathbb{F}_q^{q+1}\}$ is distributed with resepect to the Haar measure. Finite sets of states approximating the uniform Haar measure are well studied and go by the name of state t-designs [10, 11] (where $t \geq 1$ is an integer that quantifies how good the approximation is). The complete set of mutually unbiased bases described in Def. II.1 comprises a state 2-design. Numerical calculations suggest that the set $\{|J^r\rangle, r \in \mathbb{F}_q^{q+1}\}$ provides a poor approximation to a Haar-uniform distribution of pure states in $\mathbb{C}^{q^2}$. For instance, the purity of the reduced state ρ_1 in a bipartite system quantifies how entangled the bipartite state is via

---

[1] If we want our face operators to have unit trace we can solve for a more general form

$$A^r = J \sum_{B \in \mathcal{B}} |\psi_B^{rB}\rangle\langle\psi_B^{rB}| - K\mathbb{I}_q \tag{22}$$

$$\mathrm{Tr}(A^r) = J|r| - qK = 1 \tag{23}$$

$$\mathrm{Tr}\left((A^r)^2\right) = \frac{J^2(q - 1 + |r|)|r|}{q} - 2|r|JK + qK^2 = q \tag{24}$$

so that

$$J = \sqrt{\frac{q+1}{|r|}}, \quad K = \frac{-1 + \sqrt{|r|(q+1)}}{q}. \tag{25}$$

In that case we find

$$\mathrm{Tr}\left(A^r A^s\right) = q - \frac{q+1}{|r|}\Delta(r,s) \tag{26}$$

and the Hilbert-Schmidt and Fubini-Study distance measures can be derived from this.

$\frac{1}{q} \leq \mathrm{Tr}(\rho_1^2) \leq 1$ where the lower bound is saturated for maximally entangled states. A result due to Lubkin [12] states that a Haar-uniform distribution of bipartite pure states has average subsystem purity $\langle \mathrm{Tr}(\rho_1^2)\rangle_{\mathrm{Haar}} = 2q/(q^2+1)$, whereas we find

$$q = 3: \qquad \langle \mathrm{Tr}(\rho_1^2)\rangle_{\mathbb{F}_3^4} = \frac{\left(\frac{3}{9}\right) 9 + \left(\frac{7}{9}\right) 72}{3^4} = \frac{59}{81}, \tag{31}$$

which suggests that entangled states may be under-represented in $\{|J^r\rangle, r \in \mathbb{F}_q^{q+1}\}$.

The existence of a Hamming code (15) with parameters $[q+1, q-1, 3]$ means that for all prime power dimensions there exists a set of facet operators of size $|\{A\}| = q^{q-1}$ wherein any two elements obey

$$D_{HS}(A^r, A^s) \geq \sqrt{6}. \tag{32}$$

For $q = 2$ the Hamming code is simply $\mathcal{C} = \{(0,0,0),(1,1,1)\}$ and the facet operators correspond to opposite corners of a cube in the space of Hermitian operators as in Fig. 2. Using codewords of the Hamming code then the corresponding set of states obtained via Corollary IV.3 obey

$$D_{FS}(|J^r\rangle, |J^s\rangle) \geq \sqrt{\frac{6}{q}}. \tag{33}$$

As well as knowing the minimum distance $d = 3$ there exist powerful tools (e.g. weight enumerators [13]) for calculating the complete weight distribution (8) of codes such as this. In this way we can enumerate the number of states $|J^s\rangle$ at any given (discrete) distance from a particular reference state $|J^r\rangle$.

V. MUBS AND FACET OPERATORS USING THE WEYL-HEISENBERG GROUP

The starting point for Weyl-Heisenberg operators in a Hilbert space of prime power dimension $\dim(\mathcal{H}) = q$ are the operators

$$X(x)|k\rangle = |k+x\rangle, \qquad Z(z)|k\rangle = \omega^{\mathrm{tr}(kz)}|k\rangle \qquad x, z, k \in \mathbb{F}_q,\ \omega := exp(2\pi i/p), \tag{34}$$

which compose as

$$X(x)Z(z)X(x')Z(z') = \omega^{\mathrm{tr}\, x'z} X(x+x')Z(z+z'). \tag{35}$$

A Weyl-Heisenberg (generalized Pauli) operator, indexed by $x, z \in \mathbb{F}_q$, is a product of these X and Z operators. From the composition law we observe that two Weyl-Heisenberg operators commute if and only if $\mathrm{tr}(xz' - x'z) = 0$. The Weyl-Heisenberg operators generate a group that, modulo its center, has order q^2. Consider a maximal abelian subgroup of this Weyl-Heisenberg group. Then any state that is a simultaneous eigenvector of all elements of this subgroup is a stabilizer state. Gross [14] showed that in a Hilbert space of dimension $q = p^n$ there are exactly $p^n \prod_{i=1}^n (p^i + 1)$ distinct stabilizer states. Our MUB constructions below are comprised of basis vectors that are stabilizer states.

For odd prime powers, it turns out be convenient to impose a particular phase on the Weyl-Heisenberg operators so that they form the Weyl-Heisenberg group $\mathbf{D}$ of order $|\mathbf{D}| = q^2$,

$$\mathbf{D} = \{D_{x,z} := \omega^{\mathrm{tr}\,\frac{xz}{2}} X(x)Z(z) | x, z, \in \mathbb{F}_q\} \qquad \left(\text{with } \frac{\beta}{2} = 2^{-1}\beta \text{ where } 2^{-1} \in \mathbb{F}_q\right), \tag{36}$$

where individual group elements act as $D_{x,z}|k\rangle = \omega^{\mathrm{tr}\,\frac{xz}{2}+kz}|k+x\rangle$. Projectors onto rank-1 eigenstates of Weyl-Heisenberg operators (i.e., stabilizer states) can be constructed as [15, 16]

$$|\psi_B^V\rangle\langle\psi_B^V| = \frac{1}{q}\sum_{k\in\mathbb{F}_q} \omega^{\mathrm{tr}(-kV)} D_{k,kB}, \tag{37}$$

so that

$$D_{1,B}|\psi_B^V\rangle = \omega^{\mathrm{tr}(V)}|\psi_B^V\rangle, \qquad V, B \in \mathbb{F}_q. \tag{38}$$

The set of states obtained by varying Eq. (37) over all $B, V \in \mathbb{F}_q$, along with the computational basis $\mathcal{B}_\infty = \{|0\rangle, |1\rangle, \ldots\}$ is a complete set of mutually unbiased bases. One can check that the explicit form is given by

$$|\psi_B^V\rangle = \frac{1}{\sqrt{q}} \sum_{k \in \mathbb{F}_q} \omega^{\mathrm{tr}(\frac{1}{2}Bk^2 - Vk)} |k\rangle, \tag{39}$$

and this is recognizable as the Ivanovic MUB construction [2, 3]. Using the composition law Eq. (35) we can deduce

$$D_{x,z}|\psi_\infty^V\rangle\langle\psi_\infty^V|D_{x,z}^\dagger = |\psi_\infty^{V+x}\rangle\langle\psi_\infty^{V+x}|, \tag{40}$$

$$D_{x,z}|\psi_B^V\rangle\langle\psi_B^V|D_{x,z}^\dagger = \frac{1}{q}\sum_{k \in \mathbb{F}_q} \omega^{\mathrm{tr}(-kV)} D_{x,z} D_{k,kB} D_{x,z}^\dagger, \tag{41}$$

$$= \frac{1}{q}\sum_{k \in \mathbb{F}_q} \omega^{\mathrm{tr}(-k(V-z+xB))} D_{k,kB}, \tag{42}$$

$$= |\psi_B^{V-z+xB}\rangle\langle\psi_B^{V-z+xB}|. \tag{43}$$

Therefore the image of a facet operator under conjugation by a Weyl-Heisenberg operator is

$$D_{x,z} A^r D_{x,z}^\dagger = A^{r+x[1,0,\alpha,\alpha^2,\ldots,\alpha^{q-1}]-z[0,1,1,1,\ldots,1]}, \tag{44}$$

$$= A^{r+xg_1-zg_2} \quad \text{with} \quad \begin{bmatrix} 1 & 0 & \alpha & \alpha^2 & \cdots & \alpha^{q-1} \\ 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} g_1 \\ g_2 \end{bmatrix} \tag{45}$$

where g_1 and g_2 are the generators of the simplex code (a similar expression was already pointed out in the prime-dimensional case in [17]). This is a very convenient way of understanding the orbit of facet operators under conjugation by the Weyl-Heisenberg group. It is also useful to have such a concise expression for the stabilizer states involved in the construction of a facet operator (for example, such a decomposition was used in [18] to construct a witness for quantum contextuality).

For even-prime-power dimension, i.e., n qubits, it has been noted [1, 2, 19] that an Ivanovic-type MUB construction (39) over $\mathbb{F}_{q=2^n}$ will not work without modification. Instead we must move to a slightly more general structure, the Galois ring $GR(4, n)$, which has 4^n elements and its associated Teichmüller set $\mathcal{T} = \{0, 1, \xi, \xi^2, \ldots, \xi^{2^n-2}\}$ with 2^n elements. Each element $g \in GR(4, n)$ can be written $g = a + 2b$ with $a, b \in \mathcal{T}$ and the trace map $\mathrm{tr} : GR(4, n) \mapsto \mathbb{Z}_4$ is defined via

$$\mathrm{tr}(g = a + 2b) = \sum_{k=0}^{n-1} a^{2^k} + 2b^{2^k}.$$

With these definitions we arrive at a MUB construction that appears formally very similar to the odd-prime-power case (39)

$$|\psi_B^V\rangle = \frac{1}{\sqrt{2^n}} \sum_{k \in \mathcal{T}} \omega_4^{\mathrm{tr}(Bk^2)+2\,\mathrm{tr}(Vk)} |k\rangle \qquad \omega_4 := exp(2\pi i/4) = i \tag{46}$$

except now our labels are elements of $\mathcal{T}$ rather than $\mathbb{F}_q$. For the purpose of investigating geometrical relationships between face operators, the distinction between $\mathcal{T}$-valued vectors and $\mathbb{F}_{2^n}$-valued vectors is irrelevant. From the form of the MUB vectors in Eq. (46) we can identify them as stabilizer states [20], just as we had in the odd prime power case. For the even q case we do not know of a similarly concise expression for the orbit of Weyl-Heisenberg operators acting on facet operators as we had in Eq. (44) although it should be possible. The Weyl-Heisenberg orbit of any A^r with $r \in \mathcal{T}^{q+1}$ creates a simplex code e.g. for $q = 4$ we have

$$D_{x,z} A^{[0,0,\ldots,0]} D_{x,z}^\dagger = \big\{ A^r \,|\, \mathrm{tr}(r) \in (00000), (01111), (02222), (03333), (10123), (11032), (12301), (13210), \\ (20231), (21320), (22013), (23102), (30312), (31203), (32130), (33021) \big\}, \tag{47}$$

where we are using coordinates $\mathrm{tr}(r) = (\mathrm{tr}(r_\infty), \mathrm{tr}(r_1), \ldots) \in Z_4^5$ rather than $r \in \mathcal{T}^5$.

VI. THE DISCRETE WIGNER FUNCTION

It is possible to represent finite-dimensional quantum states as probability distributions over a phase space of discrete points. However, to recover all the predictions of quantum mechanics we must allow the probability distribution to

take on negative values, in other words we must use quasi-probabilities. Such descriptions are referred to as quasi-probability representations, the most famous of which is the Wigner function. Wootters introduced a method of constructing discrete Wigner functions based on finite fields wherein vectors from a complete set of MUBs were put in one-to-one correspondence with the lines of the affine plane $AG(2, \mathbb{F}_q)$ [21]. The connection with our work is that Wigner function of state ρ at some point in phase space is given by the expectation $\mathrm{Tr}(A\rho)$, where A is one of the facet operators in Def. II.2 and which go by the name phase point operators in the context of Wigner functions. The tools and terminology established in previous sections allow for an interesting interpretation of the relationship between phase point operators with each other and with quantum state space.

Wootters' discrete Wigner function (DWF) requires a set of q^2 trace-orthogonal phase point operators, which corresponds to a set of facet operators $\{A^r\}$ with pairwise Hamming distance $\Delta(r, s) = q$. We know that the codewords of $\mathcal{C}_{\text{simplex}}$ satisfy this constraint, as do the codewords of every translate $\mathcal{C}_{\text{simplex}} + w$ for fixed $w \in \mathbb{F}_q^{q+1}$. In this way we can obtain q^{q-1} different DWF by partitioning $\mathbb{F}_q^{q+1}$ into q^{q-1} cosets of the simplex code via a Slepian array as in Table I. This partitioning is a coding-theoretic restatement of the concept of q^{q-1} different "quantum nets" [21]. Hereafter, we will refer to a particular definition of DWF by its coset w, and it is understood that the MUBs used in constructing facet operators are those of Sec. V.

The Wigner function of ρ at the point $(x, z) \in \mathbb{F}_q \times \mathbb{F}_q$ in phase space is denoted $W_{x,z}(\rho)$, and is defined via

$$W_{x,z}(\rho) = \frac{1}{q} \mathrm{Tr}(A^{w+xg_1-zg_2}\rho) \qquad (\text{fixed } w \in \mathbb{F}_q^{q+1}) \tag{48}$$

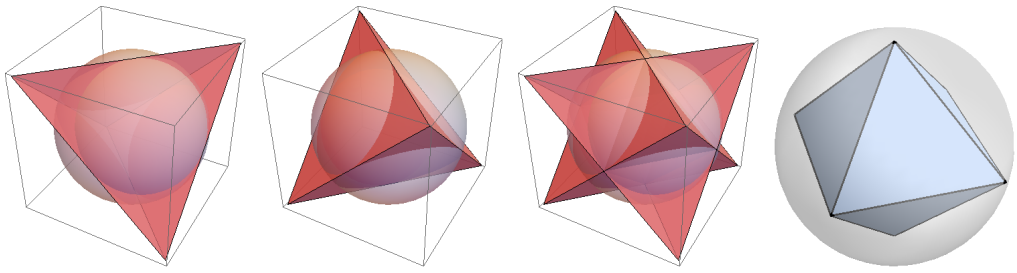
The quantity $\mathrm{Tr}(A^{w+xg_1-zg_2}\rho)$ is the Hilbert-Schmidt inner product between the operator A and the density matrix ρ, and so demanding that $W(\rho) \geq 0$ is constraining ρ to be close to A in some sense. In fact the constraints $W_{x,z}(\rho) \geq 0 \ \forall x, z \in \mathbb{F}_q$ describe a simplex in $\mathcal{H}$ with q^2 bounding facets (hence the name for facet operators). In general our construction gives

$$\text{Simplex code in Hamming space} \quad \longleftrightarrow \quad \text{Simplex in Hilbert space.} \tag{49}$$

Another geometrical object of interest is the single-particle ($q = p$) stabilizer polytope defined as the convex hull of all $p(p + 1)$ stabilizer MUB vectors $|\psi_B^V\rangle$. Cormick *et al.* [22] showed that a halfspace description of the single-qudit stabilizer polytope is given by

$$\text{Stabilizer polytope} := \{\rho | \ \mathrm{Tr}(\rho A^r) \geq 0, \forall r \in \mathbb{F}_p^{p+1}\}. \tag{50}$$

From the discussion in the previous paragraph we see that the stabilizer polytope is the intersection of all simplices associated with the simplex code and all its cosets (see Figure 2 for an illustration of the $p = 2$ case).



(a) (b) (c) (d)

FIG. 2. (a) Applying the facet operator construction to the simplex code $\mathcal{C}_{\text{simplex}}$ and (b) to a coset $\mathcal{C}_{\text{simplex}} + w$ (c) The intersection of these two simplices produces the stabilizer polytope (octahedron) (d) See also [23–25] for related geometrical discussions.

We are interested in non-negatively represented pure states, that is states $|\phi\rangle$ such that $W_{x,z}(|\phi\rangle\langle\phi|) \geq 0 \ \forall x, z \in \mathbb{F}_q$. In Figure 2(a) we see that nonegatively represented pure qubit states in the DWF with $w = (0, 0, 0)$ are those that are both (i) on the surface of the Bloch sphere, and (ii) contained within the tetrahedron. Figure 2(b) illustrates the same idea for the DWF with $w = (0, 0, 1)$. Cormick *et al.* [22] showed that the only pure states that are non-negatively represented for all q^{q-1} Wigner functions (simultaneously) are the $q(q + 1)$ stabilizer MUB states $|\psi_B^V\rangle$ used in the DWF construction and this is illustrated in Figure 2(c,d). When we move to qutrit (or any odd prime dimension) state space the story changes slightly from the qubit case we have depicted. There are now $q^{q-1} = 9$ different DWF and we are guaranteed by [22] that all $q(q + 1) = 12$ stabilizer states $|\psi_B^V\rangle$ are non-negatively represented no matter

which DWF we use. However, a result by Gross [14] says that a pure state is non-negatively represented in the DWF with $w = \vec{0}$ if *and only if* it is a stabilizer state. For qubits the set of non-negatively represented pure states is of finite measure, but for odd-prime qudits it is exactly the set of $p(p+1)$ stabilizer states. Moving on to multiple particles of odd prime dimension (q is an odd prime power) then it seems that Gross' choice of DWF is the unique one obeying the discrete version of Hudson's Theorem [14]: a pure state is non-negatively represented if and only if it is a stabilizer state. A priori we know that at least $q(q+1)$ stabilizer states will be positively represented but this only represents an exponentially small (in n) fraction of all $p^n \Pi_{i=1}^n (p^i + 1)$ stabilizer states. Hence the discrete Hudson theorem is a geometrically remarkable fact, as well as having practical relevance for questions surrounding fault-tolerant quantum computing [26, 27], resources theories [28] and contextuality [18]. To see that $w = \vec{0}$ recovers Gross' choice of DWF insert (39) into $A^{r=[0,0,\ldots,0]}$ and simplify to obtain $\sum_{k \in \mathbb{F}_q} |k\rangle\langle -k|$ i.e., the discrete parity operator (the parity operator also forms the starting point for the continuous Wigner function [29]). This particular instance of Wootters' discrete Wigner function is also singled-out by its highly symmetric properties [21, 36, 37].

We hope that our way of analyzing these Wigner simplices and their relationships with each other and with the set of quantum states will prove enlightening. In principle, we could construct a Wigner-like representation using the Alltop [30, 31] MUB vectors $|^{(a)}\phi_B^V\rangle = \frac{1}{\sqrt{q}} \sum_{k \in \mathbb{F}_q} \omega^{\mathrm{tr}(ak^3 + \frac{1}{2}Bk^2 - Vk)} |k\rangle$, which are equal to the Ivanovic MUB vectors for $a = 0$ and unitarily equivalent but highly non-stabilizer [32, 33] otherwise ($a \neq 0$). One could also apply our Wigner simplex construction to unitarily-inequivalent MUB vectors [4]. Note that Bengtsson and Ericsson [38], without restricting to stabilizer MUBs, have studied the equivalent of Wigner simplices and the stabilizer polytope (the complementarity polytope) and their relationship to quantum state space. Their construction of a simplex via mutually orthogonal Latin squares is isomorphic to our simplex code construction [7] in dimension $q = p^n$.

VII. SUMMARY

We identified a construction relating the Hamming distance between q-ary strings to the Hilbert Schmidt distance between certain Hermitian operators and the Fubini-Study distance between certain states. Any q-ary classical code of length up to $N \leq q + 1$ is suitable and our hope is that the ability to use a vast array of coding-theoretic tools (distance distributions, automorphisms etc.) will prove useful in the quantum context. The types of operators and states that our construction provides are somewhat limited so it is unlikely that our results are directly applicable to outstanding open problems like the existence of symmetric informationally-complete positive operator-valued measures (SIC-POVMs).

One topic for which our results are certainly relevant is the discrete Wigner function, where the expectation value of our operators are quasi-probabilities representing quantum states. The discrete Wigner function is both foundationally interesting as well as practically relevant for fault-tolerant quantum computing [26–28]. We showed how a famous family of maximum distance separable codes, the simplex codes, when applied via our construction, reproduce the Wigner simplex in Hilbert space. More generally, our results represent a convenient tool for working with, and a novel way of thinking about, Wootters' Wigner function in arbitrary prime-power dimension.

VIII. ACKNOWLEDGEMENTS

We thank Ingemar Bengtsson, Huangjun Zhu and Hammam Qassim for helpful comments on a previous draft. We acknowledge financial support from the Government of Canada through NSERC via the discovery grant program, as well as the U. S. Army Research Office through grant W911NF-14-1-0103, and FQXI.

[1] W. K. Wootters and B. D. Fields "Optimal state-determination by mutually unbiased measurements" Ann. Phys, **191**, 2, 363–381 (1989). http://dx.doi.org/10.1016/0003-4916(89)90322-9

[2] A. Klappenecker and M. Rötteler " Constructions of mutually unbiased bases" Finite fields and applications, 137–144 (2004) http://dx.doi.org/10.1007/978-3-540-24633-6_10

[3] I. D. Ivanović "Geometrical description of quantal state determination" J. Phys. A, **14**, 12, 3241 (1981). http://dx.doi.org/10.1088/0305-4470/14/12/019

[4] W. M. Kantor, "MUBs inequivalence and affine planes" J. Math. Phys. **53**, number 3, 032204, (2012). http://link.aip.org/link/doi/10.1063/1.3690050

[5] W. van Dam and M. Howard "Bipartite entangled stabilizer mutually unbiased bases as maximum cliques of Cayley graphs" Phys. Rev. A. **84**, 012117, (2011). http://dx.doi.org/10.1103/PhysRevA.84.012117

[6] F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error Correcting Codes', North-Holland Publishing Company (1978).

[7] R. C. Singleton, "Maximum distance q-nary codes", IEEE Trans. Inf. Theory 10 (2): 116118 (1964). http://dx.doi.org/10.1109/TIT.1964.1053661

[8] A. Jamiołkowski , "Linear transformations which preserve trace and positive semidefiniteness of operators" Rep. Math. Phys., **3**, 4, 275–278 (1972). http://dx.doi.org/10.1016/0034-4877(72)90011-0

[9] M. D. Choi, "Completely positive linear maps on complex matrices" Linear Algebra and its Applications, **10**, 3, 285–290 (1975). http://dx.doi.org/10.1016/0024-3795(75)90075-0

[10] A. Ambainis and J, Emerson, "Quantum t-designs: t-wise independence in the quantum world", CCC'07 Twenty-Second Annual IEEE Conference on Computational Complexity, 129–140, (2007). http://dx.doi.org/10.1109/CCC.2007.26

[11] G. Zauner, "Quantum Designs: Foundations of a non-commutative Design Theory", IJQI, textbf9, 1, 445–507 (2011). http://dx.doi.org/10.1142/S0219749911006776

[12] E. Lubkin, "Entropy of an n-system from its correlation with a k-reservoir" J. Math. Phys. 19, 1028 (1978) http://dx.doi.org/10.1063/1.523763

[13] D. S. Kim, "Weight Distributions of Hamming Codes (II)" arXiv:0710.1469, (2007). arXiv:0710.1469

[14] D. Gross, "Hudson's theorem for finite-dimensional quantum systems" J. Math. Phys. **47**, number 12, 122107, (2006). http://link.aip.org/link/doi/10.1063/1.2393152

[15] Gross, D. and Audenaert, K. and Eisert, J. " Evenly distributed unitaries: On the structure of unitary designs" Journal of Mathematical Physics, 48, 052104 (2007) http://dx.doi.org/10.1063/1.2716992

[16] A. Vourdas "Galois quantum systems" J. Phys. A, **38**, 39, 8453 (2005). http://dx.doi.org/10.1088/0305-4470/38/39/011

[17] D. M. Appleby, I. Bengtsson, and S. Chaturvedi, "Spectra of phase point operators in odd prime dimensions and the extended Clifford group " J. Math. Phys. **49**, 012102, (2008). http://dx.doi.org/10.1063/1.2824479

[18] M. Howard, J. Wallman, V. Veitch and J. Emerson, "Contextuality supplies the magic for quantum computation" Nature, **510** pp. 351-355 (2014).

[19] C. Godsil and A. Roy "Equiangular lines, mutually unbiased bases, and spin models" European Journal of Combinatorics, **30**, 1, 246–262 (2009). http://dx.doi.org/10.1016/j.ejc.2008.01.002

[20] J. Dehaene and B. De Moor "Clifford group, stabilizer states, and linear and quadratic operations over GF(2)" Phys. Rev. A. **68**, 4, 042318, (2003). http://dx.doi.org/10.1103/PhysRevA.68.042318

[21] K. S. Gibbons, M. J. Hoffman, and W. K. Wootters, "Discrete phase space based on finite fields" Phys. Rev. A. **70**, 062101, (2004). http://dx.doi.org/10.1103/PhysRevA.70.062101

[22] C. Cormick, E. F. Galvao, D. Gottesman, J. P. Paz, and . O. Pittenger "Classicality in discrete Wigner functions" Phys. Rev. A 73, 012301 (2006) http://dx.doi.org/10.1103/PhysRevA.73.012301

[23] E. F. Galvão "Discrete Wigner functions and quantum computational speedup" Phys. Rev. A. **71**, 4, 042302, (2005). http://dx.doi.org/10.1103/PhysRevA.71.042302

[24] D. M. Appleby, I. Bengtsson, H. B. Dang, " Galois Unitaries, Mutually Unbiased Bases, and MUB-balanced states" arXiv:1409.7987 (2014). arXiv:1409.7987

[25] W. van Dam and M. Howard "Noise thresholds for higher-dimensional systems using the discrete Wigner function" Phys. Rev. A 83, 032310 (2011)

[26] V. Veitch, C. Ferrie, D. Gross and J. Emerson, "Negative quasi-probability as a resource for quantum computation" New Journal of Physics **14**,11 pp. 113011, (2012). http://dx.doi.org/10.1088/1367-2630/14/11/113011

[27] A. Mari and J. Eisert, "Positive Wigner functions render classical simulation of quantum computation efficient" Physical review letters **109**, 23, 230503, (2012). http://dx.doi.org/10.1103/PhysRevLett.109.230503

[28] V. Veitch, S. A. H. Mousavian, D. Gottesman and J. Emerson "The resource theory of stabilizer quantum computation" New J. Phys. **16** 013009 (2014)

[29] A. Royer, "Wigner function as the expectation value of a parity operator" Phys. Rev. A. **15**, 2, 449–450, (1977). http://dx.doi.org/10.1103/PhysRevA.15.449

[30] W. O. Alltop, "Complex sequences with low periodic correlations" IEEE Trans. Inform. Theory **26** 350 1980

[31] I. Bengtsson, K. Blanchfield, E. Campbell and M. Howard, "Order 3 Symmetry in the Clifford Hierarchy" J. Phys. A: Math. Theor. **47** 455302 (2014)

[32] M. Howard, "Maximum nonlocality and minimum uncertainty using magic states", Phys. Rev. A **91**, 4, 042103 (2015). http://dx.doi.org/10.1103/PhysRevA.91.042103

[33] D. Andersson, I. Bengtsson, K. Blanchfield and H. B. Dang "States that are far from being stabilizer states" arXiv:1412.8181 (2014)

[34] H. Zhu, "Mutually unbiased bases as minimal Clifford covariant 2-designs" arXiv:1505.01123, (2015). arXiv:1505.01123

[35] C. Carmeli, J. Schultz and A. Toigo, "Covariant mutually unbiased bases" arXiv:1504.06415, (2015). arXiv:1504.06415

[36] H. Zhu, "Permutation symmetry determines the discrete Wigner function" arXiv:1504.03773, (2015). arXiv:1504.03773

[37] S. Chaturvedi, N. Mukunda and R. Simon "Wigner distributions for finite-state systems without redundant phase-point operators" J. Phys. A, **43**, 7, 075302 (2010). http://dx.doi.org/10.1088/1751-8113/43/7/075302

[38] I. Bengtsson and A. Ericsson, "Mutually Unbiased Bases and The Complementarity Polytope" Open Sys. & Information Dyn. **12** 107-120 (2005). http://dx.doi.org/10.1007/s11080-005-5721-3